



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001352319 A**(43) Date of publication of application: **21.12.01**

(51) Int. Cl.

H04L 9/08
G06F 1/00
G09C 1/00

(21) Application number: **2000126692**(71) Applicant: **MIYAJI MITSUKO**(22) Date of filing: **23.03.00**(72) Inventor: **MIYAJI MITSUKO**(54) **INTEGRATION SYSTEM**

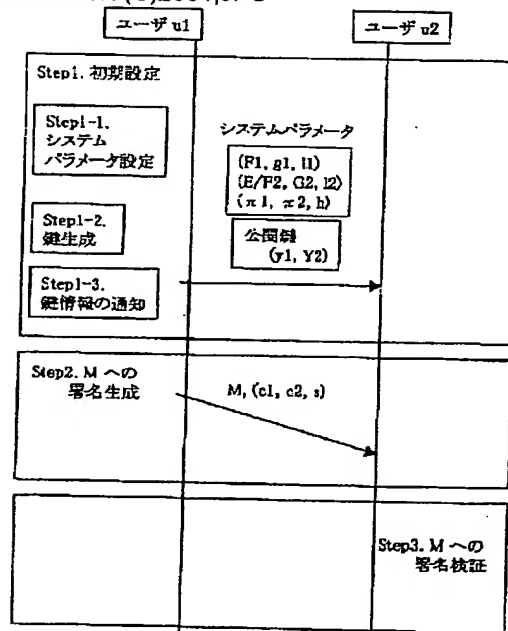
has stiffness against an attack.

(57) Abstract:

COPYRIGHT: (C)2001,JPO

PROBLEM TO BE SOLVED: To provide an integration system that relates to an encryption technology as an information security technology, especially to a key common sharing, encryption and digital signature technology, integrates a factorization problem, a discrete logarithm problem, and a discrete logarithm problem on an elliptic curve having independent security in a way that the respective securities are independent, and can provide a key common share, encryption and signature method having immunity even when one problem is attacked.

SOLUTION: The integration system adopts a key common sharing method that includes an initial setting step (1), a system parameter setting (1-1), a step (1-2) where a key for a user u1 is generated, a notice step (1-3) of key information for the user u1, a step (2) where a signature to data M by the user u1 is generated, and a step (3) where the signature to the data M by a user u2 is verified. Thus, this invention provides the key common share, encryption and signature method that



THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-352319

(P2001-352319A)

(43)公開日 平成13年12月21日(2001.12.21)

| (51)Int.Cl. ⁷ | 識別記号 | F I | キーワード*(参考) |
|--------------------------|-------|--------------|-------------------|
| H 0 4 L 9/08 | | G 0 6 F 1/00 | 3 7 0 E 5 J 1 0 4 |
| G 0 6 F 1/00 | 3 7 0 | G 0 9 C 1/00 | 6 2 0 A |
| G 0 9 C 1/00 | 6 2 0 | | 6 2 0 Z |
| | | | 6 4 0 B |
| | 6 4 0 | H 0 4 L 9/00 | 6 0 1 C |

審査請求 未請求 請求項の数18 書面 (全 10 頁) 最終頁に続く

(21)出願番号 特願2000-126692(P2000-126692)

(22)出願日 平成12年3月23日(2000.3.23)

特許法第30条第1項適用申請有り 平成11年9月24日
 社団法人電子情報通信学会開催の「電子情報通信学会技
 術研究報告」において文書をもって発表

(71)出願人 500194647

宮地 充子

石川県能美郡辰口町旭台1-50-E-41

(72)発明者 宮地 充子

石川県能美郡辰口町旭台1-50-D-34

Fターム(参考) 5J104 AA01 AA09 AA16 EA24 EA28

EA30 EA32 EA33 JA23 JA25

JA27 JA29 LA03 LA05 LA06

NA02 NA12 NA16 NA18

(54)【発明の名称】 統合装置

(57)【要約】

【目的】情報セキュリティ技術としての暗号技術に関するものであり、特に、複数の安全性の仮定を用いて実現する鍵共有、暗号及びデジタル署名技術に関するものであり、独立な安全性をもつ素因数分解問題、離散対数問題、楕円曲線上の離散対数問題等の問題を互いの安全性が独立であるように統合し、一つの問題が攻撃されても耐用可能な鍵共有、暗号、署名方法を提供することを目的とする。

【構成】

(1) 初期設定

(1-1) システムパラメータ設定

(1-2) ユーザu1の鍵生成

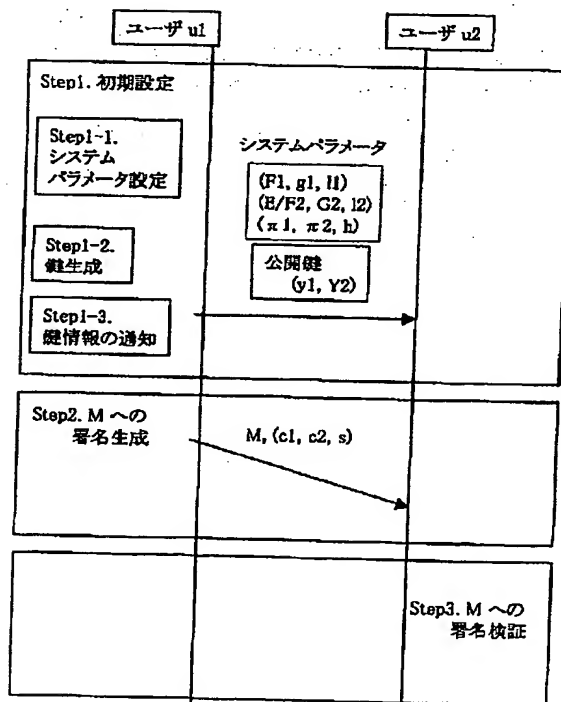
(1-3) ユーザu1の鍵情報の通知

(2) ユーザu1によるデータMへの署名生成

(3) ユーザu2によるデータMへの署名検証

の各ステップを含む鍵共有方法を用いた統合装置。

【効果】攻撃に対する頑強性をもつ鍵共有、暗号及び署名方式を与える。



【特許請求の範囲】

【請求項1】 F_1, F_2 をともに乗算が定義される有限群とし、 g_1, g_2 をそれぞれ有限群 F_1, F_2 の元とし、 g_1, g_2 は位数をそれぞれ l_1, l_2 としてもつ有限群 F_1, F_2 を用い、

ユーザ u_1 と u_2 の初期設定は、ユーザ u_1 は $0 < x_1 < l_1$ となる整数 x_1 を生成するステップと、生成した x_1 を u_1 の秘密鍵とし、秘密鍵 x_1 に対して、有限群 F_1 上で $y_1 = g_1^{(x_1)}$ を求めるステップと、求めた y_1 を公開鍵とし、公開鍵 y_1 とシステムパラメータである有限群 F_1 、元 g_1 、位数 l_1 をユーザ u_2 に通知するステップと、ユーザ u_2 は $0 < x_2 < l_2$ となる整数 x_2 を生成するステップと、生成した x_2 を u_2 の秘密鍵とし、秘密鍵 x_2 に対して、有限群 F_2 上で $y_2 = g_2^{(x_2)}$ を求めるステップと、求めた y_2 を公開鍵とし、公開鍵 y_2 とシステムパラメータである有限群 F_2 、元 g_2 、位数 l_2 をユーザ u_1 に通知するステップとからなり、ユーザ u_1 とユーザ u_2 との鍵共有は、ユーザ u_1 は $0 < k_1 < l_2$ となる乱数 k_1 を生成するステップと、生成した k_1 を用いて、有限群 F_2 上で $r_1 = g_2^{(k_1)}$ を求めるステップと、その出力 r_1 をユーザ u_2 に送信するステップと、ユーザ u_2 は $0 < k_2 < l_1$ となる乱数 k_2 を生成するステップと、生成した k_2 を用いて、有限群 F_1 上で $r_2 = g_1^{(k_2)}$ を求めるステップと、その出力 r_2 をユーザ u_1 に送信するステップと、ユーザ u_1 はユーザ u_2 より受信した r_2 と u_2 の公開鍵 y_2 及び自分の秘密鍵 x_1 及び乱数 k_1 を用いて、

$$K = (r_2^{(x_1)}, y_2^{(k_1)}) = (g_1^{(x_1 \times k_2)}, g_2^{(k_1 \times x_2)}) \in F_1 \times F_2$$

を求め、その出力 K を秘密の共有鍵とするステップと、ユーザ u_2 はユーザ u_1 より受信した r_1 と u_1 の公開鍵 y_1 及び自分の秘密鍵 x_2 及び乱数 k_2 を用いて、

$$K = (y_1^{(k_2)}, r_1^{(x_2)}) = (g_1^{(x_1 \times k_2)}, g_2^{(k_1 \times x_2)}) \in F_1 \times F_2$$

を求め、その出力 K を秘密の共有鍵とするステップとからなり、

ユーザ u_1 とユーザ u_2 がそれぞれのシステムパラメータ F_1, g_1, l_1 及び F_2, g_2, l_2 を独立に生成し、互いのシステムパラメータを用いて構成した秘密鍵 x_1, x_2 を対等に関与させることで鍵 K を共有することを特徴とする鍵共有方法。

【請求項2】 請求項1記載の鍵共有法を適用した鍵共有装置。

【請求項3】 請求項1記載の鍵共有法を実行するプログラムを記憶した記録媒体。

【請求項4】 請求項1記載の有限群 F_1, F_2 を有限体とすることを特徴とする鍵共有法。

【請求項5】 請求項1記載の有限群 F_1, F_2 を有限体の楕円曲線 $E_1 (F_1), E_2 (F_2)$ とすることを

特徴とする鍵共有法。

【請求項6】 請求項1記載の有限群 F_1, F_2 を有限体、有限体上の楕円曲線 $E_1 (F_1), E_2 (F_2)$ とすることを特徴とする鍵共有法。

【請求項7】 F_1, F_2 を有限群とし、 g_1, g_2 をそれぞれ有限群 F_1, F_2 の元とし、 g_1, g_2 の位数をそれぞれ l_1, l_2 とし、有限群 F_1, F_2 の演算をともに乗法的に表し、有限群 F_1, F_2 の元を整数に変換する写像をそれぞれ π_1, π_2 とし、有限群 F_1, F_2 、元 g_1, g_2 、位数 l_1, l_2 を格納するメモリ部を有し、有限群 F_1, F_2 の元を入力とし、その π_1, π_2 による出力を計算する演算部を有し、ユーザ u_1 は $0 < x_1 < l_1$ となる整数 x_1 及び $0 < x_2 < l_2$ となる整数 x_2 を秘密鍵として格納するメモリ部を有し、秘密鍵 x_1 に対して、有限群 F_1 上の演算で $y_1 = g_1^{(x_1)}$ を求める演算部と、秘密鍵 x_2 に対して、有限群 F_2 上の演算で $y_2 = g_2^{(x_2)}$ を求める演算部を有し、それぞれの出力 y_1, y_2 を公開鍵とし、公開鍵 y_1, y_2 とシステムパラメータである有限群 F_1, F_2 、元 g_1, g_2 、位数 l_1, l_2 、写像 π_1, π_2 を他ユーザに通知する通信部を有し、ユーザ u_1 に対して秘密にデータ M を送信したいユーザは、 $0 < k_1 < l_1$ 及び $0 < k_2 < l_2$ となる乱数 k_1, k_2 を生成し、これを格納するメモリ部を有し、有限群 F_1 上で $r_1 = g_1^{(k_1)}$ 、 $c_1 = y_1^{(k_1)}$ を、有限群 F_2 上で $r_2 = g_2^{(k_2)}$ 、 $c_2 = y_2^{(k_2)}$ を求め、

$$c = \pi_1(c_1) (+) \pi_2(c_2) (+) M$$

を求める演算部を有し、ここで (+) はビット毎の排他的論理和を表し、その出力 (r_1, r_2, c) をデータ M に対する暗号文 M とし、ユーザ u_1 に送信する通信部を有し、暗号文 (r_1, r_2, c) を受信したユーザ u_1 は、秘密鍵 x_1, x_2 を用いて、

$$M = \pi_1(r_1^{(x_1)}) (+) \pi_2(r_2^{(x_2)}) (+) c$$

を求める演算部を有し、その出力として復号文 M を入手し、ユーザ u_1 が F_1 に基づく離散対数問題と F_2 に基づく離散対数問題を対等に関与させて暗号化・復号化を行うことを特徴とする暗号化方法。

【請求項8】 請求項7記載の暗号化方法を適用した暗号装置。

【請求項9】 請求項7記載の方法を実行するプログラムを記憶した記録媒体。

【請求項10】 請求項7記載の有限群 F_1, F_2 を有限体とすることを特徴とする暗号化方法

【請求項11】 請求項7記載の有限群 F_1, F_2 を有限体上の楕円曲線 $E_1 (F_1), E_2 (F_2)$ とすることを特徴とする暗号化方法。

【請求項12】 請求項7記載の有限群 F_1, F_2 を有限体、有限体上の楕円曲線 $E_1 (F_1), E_2 (F_2)$ とすること

を特徴とする暗号化方法。

【請求項13】 F_1, F_2 を有限群とし、 g_1, g_2 をそれぞれ有限群 F_1, F_2 の元とし、 g_1, g_2 の位数をそれぞれ l_1, l_2 とし、ここで l_1 と l_2 は互いに素とし、有限群 F_1, F_2 の演算をともに乗法的に表し、有限群 F_1, F_2 の元を整数に変換する写像をそれぞれ π_1, π_2 とし、任意のビット数の整数の元をある固定されたビット数に写像するハッシュ関数を h とし、有限群 F_1, F_2 、元 g_1, g_2 、位数 l_1, l_2 を格納するメモリ部を有し、有限群 F_1, F_2 の元を入力とし、その π_1, π_2 による出力を計算する演算部と任意のビット数の整数の元を入力とし、その h による出力を計算する演算部を有し、ユーザ u_1 は $0 < x_1 < l_1$ となる整数 x_1 及び $0 < x_2 < l_2$ となる整数 x_2 を秘密鍵として格納するメモリ部を有し、秘密鍵 x_1 に対して、有限群 F_1 上の演算で $y_1 = g_1^{x_1}$ を求める演算部と、秘密鍵 x_2 に対して、有限群 F_2 上の演算で $y_2 = g_2^{x_2}$ を求める演算部を有し、それぞれの出力 y_1, y_2 を公開鍵とし、公開鍵 y_1, y_2 とシステムパラメータである有限群 F_1, F_2 、元 g_1, g_2 、位数 l_1, l_2 、写像 π_1, π_2 、 h を他ユーザに通知する通信部を有し、ユーザ u_1 が、データ M に対してデジタル署名を施してユーザ u_2 に送信したいとき、 $0 < k_1 < l_1$ 及び $0 < k_2 < l_2$ となる乱数 k_1, k_2 を生成し、これを格納するメモリ部を有し、データ M に対し $e = h(M)$ を求め、有限群 F_1 上で $r_1 = g_1^{k_1}$ を、有限群 F_2 上で $r_2 = g_2^{k_2}$ を求め、次に、 $c_1 = \pi_1(r_1) \pmod{l_1}$ 、 $c_2 = \pi_2(r_2) \pmod{l_2}$ を求め、 $s_1 = k_1^{-1} (e + x_1 c_1) \pmod{l_1}$ 、 $s_2 = k_2^{-1} (e + x_2 c_2) \pmod{l_2}$ となる $0 < s_1 < l_1 - 1$ 、 $0 < s_2 < l_2 - 1$ を求め、 $0 < s < l_1 \times l_2$ でかつ $s = s_1 \pmod{l_1}$ 、 $s = s_2 \pmod{l_2}$ となる s を求める演算部を有し、その出力 (c_1, c_2, s) をデータ M に対する署名文としてユーザ u_2 に送信する通信部を有し、署名文 (c_1, c_2, s) を受信したユーザ u_2 は、ユーザ u_1 の公開鍵及びシステムパラメータを用いて、 $e' = h(M)$ 、 $s_1' = s \pmod{l_1}$ 、 $s_2' = s \pmod{l_2}$ 、 F_1 上で $r_1' = g_1^{(e' / s_1')} y_1^{(c_1 / s_1)}$ 、 F_2 上で $r_2' = g_2^{(e' / s_2')} y_2^{(c_2 / s_2)}$ 、 $c_1' = \pi_1(r_1')$ 、 $c_2' = \pi_2(r_2')$

を求める演算部と、

$$c_1 = c_1' \pmod{l_1}, c_2 = c_2' \pmod{l_2}$$

であるか判定する判定部を有し、判定結果により署名を検証する；ユーザ u_1 が F_1 に基づく離散対数問題と F_2 に基づく離散対数問題を対等に関与させて署名生成、検証を行うことを特徴とする署名方法。

【請求項14】請求項13記載の署名方法を適用した署名装置。

【請求項15】請求項13記載の方法を実行するプログラムを記憶した記録媒体。

【請求項16】請求項13記載の有限群 F_1, F_2 を有限体とすることを特徴とする署名方法。

【請求項17】請求項13記載の有限群 F_1, F_2 を有限体上の楕円曲線 $E_1(F_1), E_2(F_2)$ とすることを特徴とする署名方法。

【請求項18】請求項13記載の有限群 F_1, F_2 を有限体、有限体上の楕円曲線 $F_1, E_2(F_2)$ とすることを特徴とする署名方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は情報セキュリティ技術としての暗号技術に関するものであり、特に、複数の安全性の仮定を用いて実現する鍵共有、暗号及びデジタル署名技術に関するものである。

【0002】

【従来の技術】秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名方式には公開鍵暗号とよばれる暗号方式を用いる。公開鍵暗号は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。簡単に説明すると、これは暗号化鍵と復号化鍵が異なり、復号化鍵は秘密にするが、暗号化鍵を公開する方式である。この公開鍵暗号の安全性の根拠に用いられるものに離散対数問題がある。離散対数問題には代表的に、有限体上定義されるもの及び楕円曲線上定義されるものがある。これはニールコブリッツ著「アコースイン ナンバア セオリイ アンド クリプトグラフィ」(Neal Koblitz, "A Course in Number theory and Cryptography", Springer-Verlag, 1987)に詳しく述べられている。楕円曲線上の離散対数問題を以下に述べる。

【0003】楕円曲線上の離散対数問題

$E(F_p)$ を有限体 F_p 上定義された楕円曲線 E とし、 E の位数が大きな素数で割れる元 G をベースポイントとする。このとき、 E の与えられた元 Y に対して、

$$Y = xG$$

となる整数 x が存在するならば x を求めよ。

【0004】以下に上記楕円曲線上の離散対数問題を応用したDSA署名をまず述べる。

従来例1

図3は従来例である楕円曲線上のDSA署名方式の構成をしめすものである。以下同図を参照しながら従来例の手順を説明する。

(1) 初期設定

有限体 F 上の楕円曲線を E とし、その素数位数 q の元を G 、楕円曲線の元 $E(F)$ を整数に対応させる写像を π 、任意長の整数をある固定された長さに写すハッシュ関数を h とする。ユーザ u_1 の公開鍵を $Y_a = x_a G$ とし、秘密鍵を x_a とする。 u_1 の公開鍵とともに、楕円曲線 E/F 、ベースポイント G 、写像 π 、 h をシステムパラメータとして公開する。

【0005】(2) メッセージ M に対するユーザ u_1 の署名生成

1. $e = h(M)$ を計算する。
2. 乱数 $0 < k < q$ を生成する。
3. $R_1 = kG$, $c_1 = \pi(R_1) \pmod{q}$, $s = k^{-1}(e + c_1 x_a) \pmod{q}$ を計算する。ここで $c_1 = 0$ あるいは $s = 0$ であればもう一度、2に戻って k をとり直す。
4. (c_1, s) を署名として M とともに送信する。

【0006】(3) 署名検証

1. $e = h(M)$ を計算する。
2. $c_1 = 0$ あるいは $s = 0$ であれば、NGを出力。
3. $R_1' = e/sG + c_1/sY$, $c_1' = \pi(R_1')$ を計算する。
4. $c_1 = c_1' \pmod{q}$ であればOKを出力し、そうでないときはNGを出力する。

【0007】上記従来例1では、一つの楕円曲線 E の離散対数問題に安全性に依存している。このため、利用している楕円曲線 E 上の離散対数問題が攻撃できると、ユーザの署名方式の安全性が損なわれることになる。ユーザがクライアントの位置付けであれば、被害は小さいかもしれないが、例えばサーバであったり公開鍵証明書発行局であるなど公的な位置付けの機関の方式が解読されると被害が非常に大きい。

【0008】ところが、楕円曲線の離散対数問題では、特定の楕円曲線に対して適用可能な攻撃が提案されるなど、一つの楕円曲線に依存したシステムの安全性が指摘されている。これについては以下の論文が詳しい。

A. Menezes, T. Okamoto and S. Vanstone, 'Reducing elliptic curve logarithms to logarithms in a finite field', IEEE Transactions on

Information Theory, 39 (1993), 1639-1646.

T. Satoh and K. Araki, 'Fermat quotients and the polynomial time discrete logarithm algorithm for anomalous elliptic curve', Commentarii Math. Univ. St. Pauli., vol. 47 (1988), 81-92.

【0009】次に有限体上の離散対数問題を利用した鍵共有方式を従来例としてあげる。

従来例2

図4は従来例である有限体上のDH鍵共有方式の構成をしめすものである。以下同図を参照しながら従来例の手順を説明する。

(1) 初期設定

有限体 F の素数位数 q の元を g とする。ユーザ u_1 の秘密鍵を x_a 、公開鍵を $y_a = g^{x_a}$ とし、ユーザ u_2 の秘密鍵を x_b 、公開鍵を $y_b = g^{x_b}$ とする。ユーザの公開鍵とともに、有限体 F 、ベースポイント g 、位数 q をシステムパラメータとして公開する。

【0010】(2) 鍵共有

ユーザ u_1 は、

1. 乱数 $0 < k_a < q$ を生成する。
2. 有限体 F 上で、

$$r_1 = g^{k_a}$$

を計算し、 u_2 に送信する。ユーザ u_2 は、

3. 乱数 $0 < k_b < q$ を生成する。
4. 有限体 F 上で、

$$r_2 = g^{k_b}$$

を計算し、 u_1 に送信する。

ユーザ u_1 は、

5. 受信した r_2 と u_2 の公開鍵 y_b と自分の秘密鍵 x_a と乱数 k_a を用いて、有限体 F 上で、

$$K = (r_2^{x_a}, y_b^{k_a}) = (g^{(k_b \times x_a)}, g^{(k_a \times x_b)}) \in F \times F$$

を計算し、共有鍵 K を得る。ユーザ u_2 は、

6. 受信した r_1 と u_1 の公開鍵 y_a と自分の秘密鍵 x_b と乱数 k_b を用いて、有限体 F 上で、

$$K = (y_a^{k_b}, r_1^{x_b}) = (g^{(k_b \times x_a)}, g^{(k_a \times x_b)}) \in F \times F$$

を計算し、共有鍵 K を得る。

【0011】従来例2で見たように、鍵共有を実現したいユーザはともに同じシステムパラメータを共有し、そのシステムパラメータ上で公開鍵と秘密鍵のペアを生成し、共有鍵の安全性も利用した1つのシステムパラメータに依存する。しかしながら、異なるユーザの間で同じシステムパラメータの利用を強制することは、ユーザの利便性を損なう。また、安全性の観点からも従来例1で述べたように、1つのシステムパラメータに依存してい

るので、このパラメータが解読されると両ユーザのシステムパラメータを変更しなければならないという問題を持つ。

【0012】

【発明が解決しようとする課題】公開鍵暗号を用いた暗号方式、鍵共有方式、署名方式では、攻撃に対して、可能な限り強力に構成することが必須である。従来例の暗号方式、鍵共有方式、署名方式においては、安全性の根拠を離散対数問題や素因数分解という一つの問題（システムパラメータと呼ばれる）に帰着している。しかしながら、この方法では、安全性を帰着している問題が攻撃された場合、その方式で構成されたすべてのデータが攻撃されることになる。特に、近年楕円曲線上の離散対数問題の攻撃に見られるように、特定の楕円曲線上の離散対数問題が攻撃されるなど、1つの方式に安全性を帰着させたシステムは、攻撃に対して非常に弱いという欠点がある。

【0013】また、ユーザが自由にシステムパラメータを生成し決定できる方が、より汎用的でかつ安全な方式を与える。しかし鍵共有方式においては、従来例2で見たように、同じシステムパラメータ上での計算を要求するので、事前に同じシステムパラメータ上で公開鍵、秘密鍵のペアを生成する必要がある。また、上述と同様に、利用したシステムパラメータに基づく問題が攻撃されると、安全性が損なわれるという問題がある。

【0014】本発明は、この従来例における問題点を鑑みて行なわれたもので、独立な安全性をもつ素因数分解、離散対数問題、楕円曲線上の離散対数問題などのシステムパラメータを互いの安全性が独立であるように統合し、攻撃されても耐用可能な鍵共有、暗号、署名方法を提供することを目的とする。

【0015】

【課題を解決するための手段】本発明は上述の問題点を解決するため、請求項1では、 F_1 、 F_2 をともに乗算が定義される有限群とし、 g_1 、 g_2 をそれぞれ有限群 F_1 、 F_2 の元とし、 g_1 、 g_2 は位数をそれぞれ l_1 、 l_2 としてもつ有限群 F_1 、 F_2 を用い、ユーザ u_1 と u_2 の初期設定は、ユーザ u_1 は $0 < x_1 < l_1$ となる整数 x_1 を生成するステップと、生成した x_1 を u_1 の秘密鍵とし、秘密鍵 x_1 に対して、有限群 F_1 上で $y_1 = g_1^{x_1}$ を求めるステップと、求めた y_1 を公開鍵とし、公開鍵 y_1 とシステムパラメータである有限群 F_1 、元 g_1 、位数 l_1 をユーザ u_2 に通知するステップと、ユーザ u_2 は $0 < x_2 < l_2$ となる整数 x_2 を生成するステップと、生成した x_2 を u_2 の秘密鍵とし、秘密鍵 x_2 に対して、有限群 F_2 上で $y_2 = g_2^{x_2}$ を求めるステップと、求めた y_2 を公開鍵とし、公開鍵 y_2 とシステムパラメータである有限群 F_2 、元 g_2 、位数 l_2 をユーザ u_1 に通知するステップとからなり、ユーザ u_1 とユーザ u_2 との鍵共有は、

ユーザ u_1 は $0 < k_1 < l_2$ となる乱数 k_1 を生成するステップと、生成した k_1 を用いて、有限群 F_2 上で $r_1 = g_2^{k_1}$ を求めるステップと、その出力 r_1 をユーザ u_2 に送信するステップと、ユーザ u_2 は $0 < k_2 < l_1$ となる乱数 k_2 を生成するステップと、生成した k_2 を用いて、有限群 F_1 上で $r_2 = g_1^{k_2}$ を求めるステップと、その出力 r_2 をユーザ u_1 に送信するステップと、ユーザ u_1 はユーザ u_2 より受信した r_2 と u_2 の公開鍵 y_2 及び自分の秘密鍵 x_1 及び乱数 k_1 を用いて、

$K = (r_2^{x_1}, y_2^{k_1}) = (g_1^{x_1 \times k_2}, g_2^{k_1 \times x_2}) \in F_1 \times F_2$ を求め、その出力 K を秘密の共有鍵とするステップと、ユーザ u_2 はユーザ u_1 より受信した r_1 と u_1 の公開鍵 y_1 及び自分の秘密鍵 x_2 及び乱数 k_2 を用いて、 $K = (y_1^{k_2}, r_1^{x_2}) = (g_1^{x_1 \times k_2}, g_2^{k_1 \times x_2}) \in F_1 \times F_2$ を求め、その出力 K を秘密の共有鍵とするステップとからなり、ユーザ u_1 とユーザ u_2 がそれぞれのシステムパラメータ F_1 、 g_1 、 l_1 及び F_2 、 g_2 、 l_2 を独立に生成し、互いのシステムパラメータを用いて構成した秘密鍵 x_1 、 x_2 を対等に関与させることで鍵 K を共有することを特徴とする鍵共有方法としている。

【0016】請求項2では、請求項1記載の鍵共有法を適用した鍵共有装置としている。

【0017】請求項3では、請求項1記載の鍵共有法を実行するプログラムを記憶した記録媒体としている。

【0018】請求項4では、請求項1記載の有限群 F_1 、 F_2 を有限体とすることを特徴とする鍵共有法としている。

【0019】請求項5では、請求項1記載の有限群 F_1 、 F_2 を有限体上の楕円曲線 E_1 (F_1)、 E_2 (F_2)とすることを特徴とする鍵共有法としている。

【0020】請求項6では、請求項1記載の有限群 F_1 、 F_2 を有限体、有限体上の楕円曲線 F_1 、 E_2 (F_2)とすることを特徴とする鍵共有法としている。

【0021】請求項7では、 F_1 、 F_2 を有限群とし、 g_1 、 g_2 をそれぞれ有限群 F_1 、 F_2 の元とし、 g_1 、 g_2 の位数をそれぞれ l_1 、 l_2 とし、有限群 F_1 、 F_2 の演算をともに乗法的に表し、有限群 F_1 、 F_2 の元を整数に変換する写像をそれぞれ π_1 、 π_2 とし、有限群 F_1 、 F_2 、元 g_1 、 g_2 、位数 l_1 、 l_2 を格納するメモリ部を有し、有限群 F_1 、 F_2 の元を入力とし、その π_1 、 π_2 による出力を計算する演算部を有し、ユーザ u_1 は $0 < x_1 < l_1$ となる整数 x_1 及び $0 < x_2 < l_2$ となる整数 x_2 を秘密鍵として格納するメモリ部を有し、秘密鍵 x_1 に対して、有限群 F_1 上の演算で $y_1 = g_1^{x_1}$ を求める演算部と、秘密鍵 x_2 に対して、有限群 F_2 上の演算で $y_2 = g_2^{x_2}$ を求める演算部を有し、それぞれの出力 y_1 、 y_2

を公開鍵とし、公開鍵 y_1, y_2 とシステムパラメータである有限群 F_1, F_2 , 元 g_1, g_2 , 位数 l_1, l_2 , 写像 π_1, π_2 を他ユーザに通知する通信部を有し、ユーザ u_1 に対して秘密にデータ M を送信したいユーザは、 $0 < k_1 < l_1$ 及び $0 < k_2 < l_2$ となる乱数 k_1, k_2 を生成し、これを格納するメモリ部を有し、有限群 F_1 上で $r_1 = g_1^{(k_1)}$, $c_1 = y_1^{(k_1)}$ を、有限群 F_2 上で $r_2 = g_2^{(k_2)}$, $c_2 = y_2^{(k_2)}$ を求め、

$c = \pi_1(c_1) (+) \pi_2(c_2) (+) M$

を求める演算部を有し、ここで $(+)$ はビット毎の排他的論理和を表し、その出力 (r_1, r_2, c) をデータ M に対する暗号文 M とし、ユーザ u_1 に送信する通信部を有し、暗号文 (r_1, r_2, c) を受信したユーザ u_1 は、秘密鍵 x_1, x_2 を用いて、

$M = \pi_1(r_1^{(x_1)}) (+) \pi_2(r_2^{(x_2)}) (+) c$

を求める演算部を有し、その出力として復号文 M を入手し、ユーザ u_1 が F_1 に基づく離散対数問題と F_2 に基づく離散対数問題を対等に関連させて暗号化・復号化を行うことを特徴とする暗号化方法としている。

【0022】請求項8では、請求項7記載の暗号化方法を適用した暗号装置としている。

【0023】請求項9では、請求項7記載の方法を実行するプログラムを記憶した記録媒体としている。

【0024】請求項10では、請求項7記載の有限群 F_1, F_2 を有限体とすることを特徴とする暗号化方法としている。

【0025】請求項11では、請求項7記載の有限群 F_1, F_2 を有限体上の楕円曲線 $E_1(F_1), E_2(F_2)$ とすることを特徴とする暗号化方法としている。

【0026】請求項12では、請求項7記載の有限群 F_1, F_2 を有限体、有限体上の楕円曲線 $F_1, E_2(F_2)$ とすることを特徴とする暗号化方法としている。

【0027】請求項13では、 F_1, F_2 を有限群とし、 g_1, g_2 をそれぞれ有限群 F_1, F_2 の元とし、 g_1, g_2 の位数をそれぞれ l_1, l_2 とし、ここで l_1 と l_2 は互いに素とし、有限群 F_1, F_2 の演算とともに乗法的に表し、有限群 F_1, F_2 の元を整数に変換する写像をそれぞれ π_1, π_2 とし、任意のビット数の整数の元をある固定されたビット数に写像するハッシュ関数を h とし、有限群 F_1, F_2 , 元 g_1, g_2 , 位数 l_1, l_2 を格納するメモリ部を有し、有限群 F_1, F_2 の元を入力とし、その π_1, π_2 による出力を計算する演算部と任意のビット数の整数の元を入力とし、その h による出力を計算する演算部を有し、ユーザ u_1 は $0 < x_1 < l_1$ となる整数 x_1 及び $0 < x_2 < l_2$ となる整数 x_2 を秘密鍵として格納するメモリ部を有し、秘密鍵 x_1 に対して、有限群 F_1 上の演算で $y_1 = g_1^{(x_1)}$ を求める演算部と、秘密鍵 x_2 に対して、有限

群 F_2 上の演算で $y_2 = g_2^{(x_2)}$ を求める演算部を有し、それぞれの出力 y_1, y_2 を公開鍵とし、公開鍵 y_1, y_2 とシステムパラメータである有限群 F_1, F_2 , 元 g_1, g_2 , 位数 l_1, l_2 , 写像 π_1, π_2, h を他ユーザに通知する通信部を有し、ユーザ u_1 が、データ M に対してデジタル署名を施してユーザ u_2 に送信したいとき、 $0 < k_1 < l_1$ 及び $0 < k_2 < l_2$ となる乱数 k_1, k_2 を生成し、これを格納するメモリ部を有し、データ M に対し $e = h(M)$ を求め、有限群 F_1 上で $r_1 = g_1^{(k_1)}$ を、有限群 F_2 上で $r_2 = g_2^{(k_2)}$ を求め、次に、 $c_1 = \pi_1(r_1) \pmod{l_1}$, $c_2 = \pi_2(r_2) \pmod{l_2}$ を求め、

$s_1 = k_1^{(-1)} \cdot (e + x_1 c_1) \pmod{l_1}$

$s_2 = k_2^{(-1)} \cdot (e + x_2 c_2) \pmod{l_2}$

となる $0 < s_1 < l_1 - 1, 0 < s_2 < l_2 - 1$ を求め、

$0 < s < l_1 \times l_2$ でかつ $s = s_1 \pmod{l_1},$

$s = s_2 \pmod{l_2}$

となる s を求める演算部を有し、その出力 (c_1, c_2, s) をデータ M に対する署名文としてユーザ u_2 に送信する通信部を有し、署名文 (c_1, c_2, s) を受信したユーザ u_2 は、ユーザ u_1 の公開鍵及びシステムパラメータを用いて、

$e' = h(M),$

$s_1' = s \pmod{l_1}, s_2' = s \pmod{l_2},$

F_1 上で $r_1' = g_1^{(e' / s_1')} y_1^{(c_1 / s_1)},$

F_2 上で $r_2' = g_2^{(e' / s_2')} y_2^{(c_2 / s_2)},$

$c_1' = \pi_1(r_1'), c_2' = \pi_2(r_2')$

を求める演算部と、

$c_1 = c_1' \pmod{l_1}, c_2 = c_2' \pmod{l_2}$

であるか判定する判定部を有し、判定結果により署名を検証する、ユーザ u_1 が F_1 に基づく離散対数問題と F_2 に基づく離散対数問題を対等に関連させて署名生成、検証を行うことを特徴とする署名方法としている。

【0028】請求項14では、請求項13記載の署名方法を適用した署名装置としている。

【0029】請求項15では、請求項13記載の方法を実行するプログラムを記憶した記録媒体としている。

【0030】請求項16では、請求項13記載の有限群 F_1, F_2 を有限体とすることを特徴とする署名方法としている。

【0031】請求項17では、請求項13記載の有限群 F_1, F_2 を有限体上の楕円曲線 $E_1(F_1), E_2$

(F2)とすることを特徴とする署名方法としている。

【0032】請求項18では、請求項13記載の有限群F1、F2を有限体、有限体上の楕円曲線F1、E2(F2)とすることを特徴とする署名方法としている。

【0033】

【実施例1】図1は、有限体上の離散対数問題と楕円曲線上の離散対数問題を用いた署名方法を示すものである。以下同図を参照しながら署名方法を説明する。

Step 1. 初期設定

step 1-1. システムパラメータ設定

F1、E/F2を有限体、有限体上の楕円曲線、 g_1 、 G_2 をそれぞれF1、E(F2)の元、 g_1 、 G_2 の位数をそれぞれ l_1 、 l_2 、ここで l_1 と l_2 は互いに素とし、有限体F1、楕円曲線E(F2)の元を整数に変換する写像をそれぞれ π_1 、 π_2 、任意のビット数の整数の元をある固定されたビット数に写像するハッシュ関数 h を設定する。

step 1-2. ユーザu1の鍵生成

ユーザu1は $0 < x_1 < l_1$ となる整数 x_1 及び $0 < x_2 < l_2$ となる

整数 x_2 を秘密鍵として格納し、秘密鍵 x_1 に対して、F1上で $y_1 = g_1^{x_1}$ 、秘密鍵 x_2 に対して、E(F2)上で $Y_2 = (x_2) \cdot G_2$ を求め、それぞれの出力 y_1 、 Y_2 を公開鍵とする。

step 1-3. ユーザu1の鍵情報の通知

公開鍵 y_1 、 Y_2 とシステムパラメータであるF1、E(F2)、 g_1 、 G_2 、 l_1 、 l_2 、 π_1 、 π_2 、 h を他ユーザに通知する。

【0034】Step 2. ユーザu1によるデータMへの署名生成

$0 < k_1 < l_1$ 及び $0 < k_2 < l_2$ となる乱数 k_1 、 k_2 を生成し、データMに対し $e = h(M)$ を求め、有限体F1上で $r_1 = g_1^{k_1}$ を、楕円曲線E(F2)上で $R_2 = (k_2) \cdot G_2$ を求め、次に、 $c_1 = \pi_1(r_1) \pmod{l_1}$ 、 $c_2 = \pi_2(R_2) \pmod{l_2}$ を求め、

$s_1 = k_1^{-1} (e + x_1 c_1) \pmod{l_1}$

$s_2 = k_2^{-1} (e + x_2 c_2) \pmod{l_2}$

となる $0 < s_1 < l_1 - 1$ 、 $0 < s_2 < l_2 - 1$ を求め、

$0 < s < l_1 \times l_2$ でかつ $s = s_1 \pmod{l_1}$ 、 $s = s_2 \pmod{l_2}$

となる s を求める。その出力 (c_1, c_2, s) をデータMに対する署名文としてユーザu2に送信する。

【0035】Step 3. ユーザu2によるデータMへの署名検証ユーザu1の公開鍵及びシステムパラメータを用いて、

$e' = h(M)$ 、

$s_1' = s \pmod{l_1}$ 、 $s_2' = s \pmod{l_2}$ 、

F1上で $r_1' = g_1^{s_1'} (e' / s_1') y_1^{c_1} / s_1$ 、

E(F2)上で $R_2' = (e' / s_2') G_2 + (c_2 / s_2) Y_2$ 、

$c_1' = \pi_1(r_1')$ 、 $c_2' = \pi_2(R_2')$

を求め、

$c_1 = c_1' \pmod{l_1}$ 、 $c_2 = c_2' \pmod{l_2}$

ならば、正しい署名と判定し、そうでなければ署名を拒絶する。

【0036】上記実施例1は、異なる独立な安全性を持つ2つの署名方式を対等に関与させた署名方式となっている。つまり、有限体F1上の離散対数問題と楕円曲線E/F2上の離散対数問題に対して、step1において、それぞれの群上で公開鍵と秘密鍵のペアを生成し、step2において両方の秘密情報を対等に、すなわち主従、あるいは時系列的な順序なく関与させて、署名の生成を行っている。この結果、仮に1つの署名方式の安全性が損なわれても、署名方式の安全性はもう一方の署名方式で保たれることが可能になる。

【0037】実施例1では、有限体上の離散対数問題と楕円曲線上の離散対数問題の2つを統合した署名方式となっているが、実施例はこれに限定されない。例えばRSA、有限体上の離散対数問題、楕円曲線上の離散対数問題など、安全性の異なる2つ以上の方式を独立に対等に統合することにより、安全性を強化することも含まれる。また言うまでもなく、本実施例では、DSA署名ベースの統合を行っているが、それ以外の署名、schnorr署名、Nyberg-Rueppel署名など、異なる署名方式の統合も含まれる。

【0038】

【実施例2】図2は、有限体上の離散対数問題と楕円曲線上の離散対数問題を用いた鍵共有方法を示すものである。以下同図を参照しながら署名方法を説明する。

Step 1. 初期設定

Step 1-1. ユーザu1の鍵生成

ユーザu1は、F1を有限体、 g_1 をF1の元とし、その位数 l_1 に対して、 $0 < x_1 < l_1$ となる整数 x_1 を生成し、F1上で $y_1 = g_1^{x_1}$ を求め、求めた y_1 を公開鍵、生成した x_1 をu1の秘密鍵とし、公開鍵 y_1 とシステムパラメータであるF1、元 g_1 、位数 l_1 をユーザu2に通知する。

step1-2. ユーザu2の鍵生成

ユーザu2は、E(F2)を有限体上の楕円曲線、 G_2 をE(F2)の元とし、その位数 l_2 に対し、 $0 < x_2 < l_2$ となる整数 x_2 を生成し、E(F2)上で $Y_2 = (x_2) \cdot G_2$ を求め、求めた Y_2 を公開鍵、生成した x_2 をu2の秘密鍵とし、公開鍵 Y_2 とシステムパラメータ

タである $E(F_2)$ 、元 G_2 、位数 l_2 をユーザ u_1 に通知する。

【0039】Step 2. ユーザ u_1 とユーザ u_2 との鍵共有

step 2-1. ユーザ u_1 の処理

ユーザ u_1 は $0 < k_1 < l_2$ となる乱数 k_1 を生成し、 $E(F_2)$ 上で $R_1 = (k_1)G_2$ を求め、その出力 R_1 をユーザ u_2 に送信する。

step 2-2. ユーザ u_2 の処理

ユーザ u_2 は $0 < k_2 < l_1$ となる乱数 k_2 を生成し、 F_1 上で $r_2 = g_1^{(k_2)}$ を求め、その出力 r_2 をユーザ u_1 に送信する。

step 2-3. ユーザ u_1 の鍵共有処理

ユーザ u_1 はユーザ u_2 より受信した r_2 と u_2 の公開鍵 y_2 及び自分の秘密鍵 x_1 及び乱数 k_1 を用いて、 $K = (r_2^{(x_1)}, (k_1)Y_2) = (g_1^{(x_1 \times k_2)}, (k_1 \times x_2)G_2) \in F_1 \times E(F_2)$ を求め、その出力 K を秘密の共有鍵とする。

step 2-4. ユーザ u_2 の鍵共有処理

ユーザ u_2 はユーザ u_1 より受信した r_1 と u_1 の公開鍵 y_1 及び自分の秘密鍵 x_2 及び乱数 k_2 を用いて、 $K = (y_1^{(k_2)}, (x_2)R_1) = (g_1^{(x_1 \times k_2)}, (k_1 \times x_2)G_2) \in F_1 \times E(F_2)$ を求め、その出力 K を秘密の共有鍵とする。

【0040】上記実施例2は、各ユーザが独立な安全性を持つ群を生成し、それらを対等に関与させた鍵共有方法となっている。つまり各ユーザは、それぞれ有限体 F_1 上の離散対数問題と楕円曲線 E/F_2 上の離散対数問題に対して、step 1において、各ユーザの利用する群上で公開鍵と秘密鍵のペアを独立に生成し、step 2において両方の秘密情報を対等に、すなわち主従、あるいは時系列的な順序なく関与させて、鍵共有を行っている。この結果、各ユーザは、鍵共有を行うユーザ間で、同じシステムパラメータを用いて公開鍵と秘密鍵を生成する必要なく鍵共有が可能になり、ユーザの利便性が図られている。さらに、仮に一方のユーザの方式の安

全性が損なわれても、鍵共有方式の安全性はもう一方のユーザの方式で保たれることが可能になり、安全性が強化されている。

【0041】実施例2では、有限体上の離散対数問題と楕円曲線上の離散対数問題の2つを統合した鍵共有方式となっているが、実施例はこれに限定されない。例えば、有限体上の離散対数問題、楕円曲線上の離散対数問題の安全性の異なる2つ以上の方式を独立に対等に統合することにより、安全性を強化することも含まれる。

【0042】

【発明の効果】以上に説明したように本発明は、従来例における問題点、すなわち従来の暗号方式、鍵共有方式、署名方式では、安全性の根拠を離散対数問題や素因数分解という一つの問題に帰着させているため、安全性を帰着している問題が攻撃された場合、その方式で構成されたすべてのデータが攻撃されることになる。すなわち、攻撃に対する頑強性を持たない。特に、鍵共有方式においては、従来例2で見たように、ユーザ間で同じシステムパラメータを用いて公開鍵、秘密鍵のペアを生成する必要があり、汎用性が損なわれるという問題があった。

【0043】本発明は、この従来例における問題点を鑑みて行なわれたもので、独立な安全性をもつ問題を互いの安全性が独立であるように統合し、一つの問題が攻撃されても耐用可能な鍵共有、暗号、署名方法を提供することを目的とする。特に、鍵共有においては、ユーザが自由にシステムパラメータを設定することを可能にし、汎用性と利便性を実現した鍵共有、暗号、署名方法を提供することを目的にする。安全で汎用的な暗号方式、鍵共有方式、署名方法を提供することができ、その実用的価値は大きい。

【図面の簡単な説明】

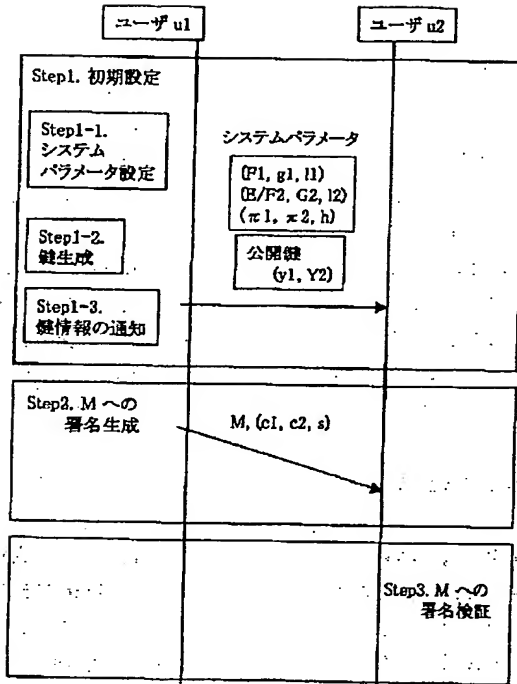
【図1】実施例1の署名装置の構成図

【図2】実施例2の鍵共有装置の構成図

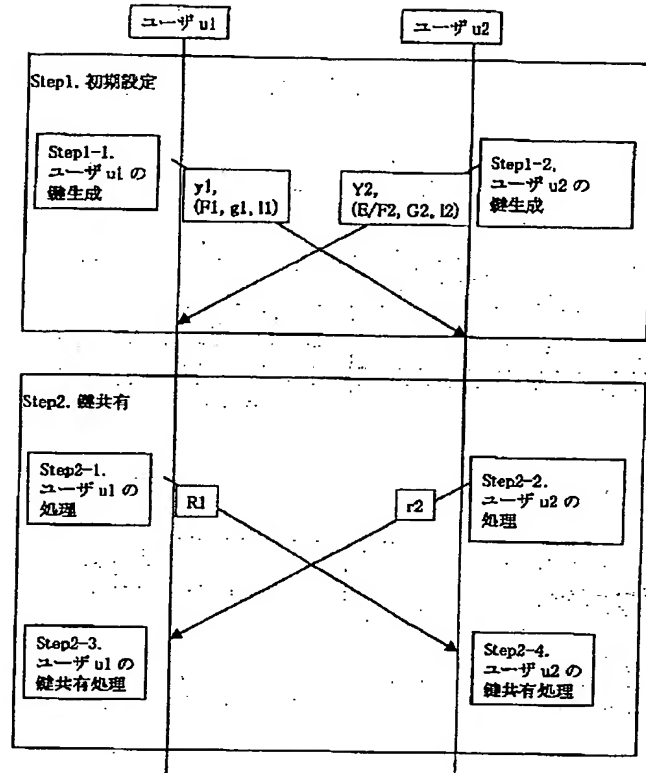
【図3】従来例1の楕円曲線上のDSA署名の構成図

【図4】従来例2の有限体上の鍵共有装置の構成図。

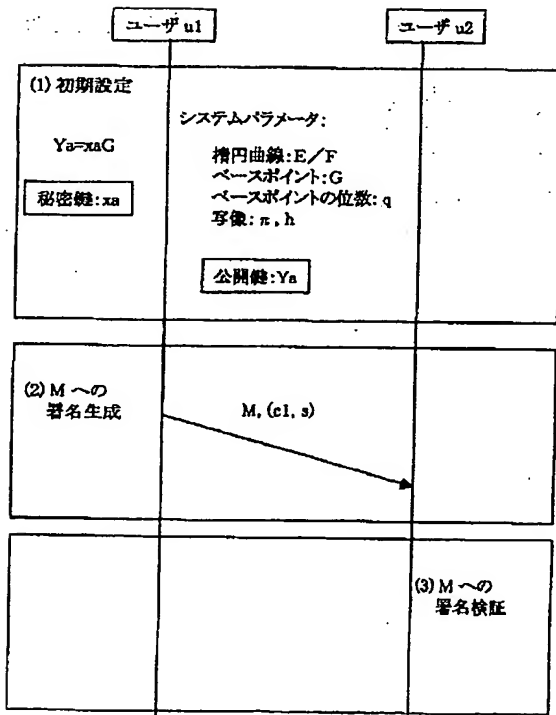
【図1】



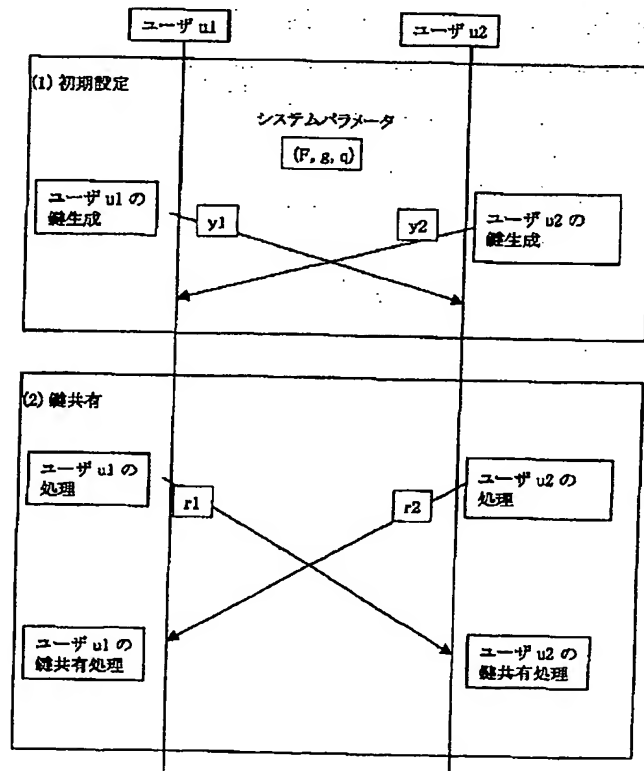
【図2】



【図3】



【図4】



フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

テーマコード(参考)

H 0 4 L 9/00

6 0 1 E